БЕЗОПАСНОСТЬ БАЗ ДАННЫХ

ФИО преподавателя: Селин А.А., канд. техн. наук

ЗАЩИТА ДАННЫХ НА ОСНОВАНИИ НАДЕЖНОГО КОМПОНЕНТА ПЕРЕДНЕГО ПЛАНА

Учебные вопросы:

1. Каналы утечки в многозначной подсистеме защиты баз данных
2. Архитектура SD-DBMS с переадресацией запросов
3. Архитектура с тиражированием

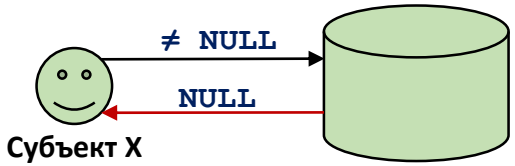
КАНАЛЫ УТЕЧКИ В МНОГОЗНАЧНОЙ ПОДСИСТЕМЕ ЗАЩИТЫ БАЗ ДАННЫХ

Канал утечки – это механизм, посредством которого субъект, обладающий высоким уровнем благонадежности, может предоставлять информацию менее благонадежным субъектам.

Виды каналов утечки (косвенных каналов):

Каналы утечки памяти

Маскирование данных с высокой СКД значениями NULL – запись в защищенную область конкретного значения с последующим чтением оттуда опять значения NULL (явное указание на факт сокрытия данных – основание для применения средств взлома базы данных)

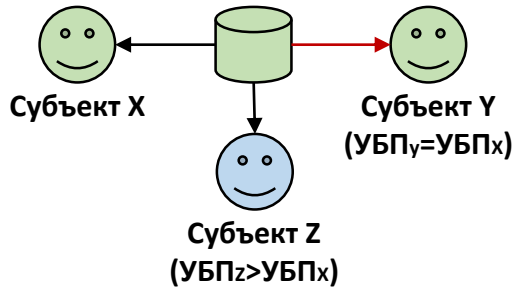


Если субъект X получил доступ в соответствии со своим уровнем благонадежности пользователя к данным с некоторой степенью конфиденциальности, то ему ничто не помешает передать эти данные субъекту Y с более низким уровнем благонадежности.

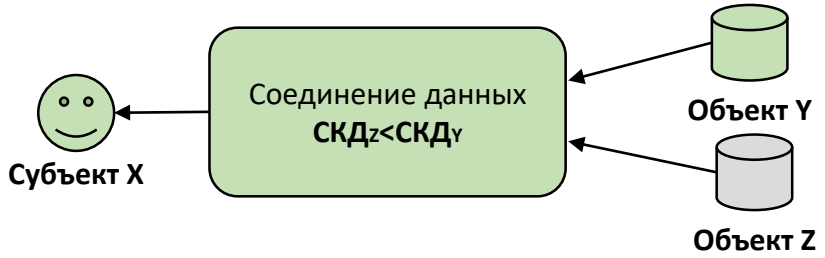
КАНАЛЫ УТЕЧКИ В МНОГОЗНАЧНОЙ ПОДСИСТЕМЕ ЗАЩИТЫ БАЗ ДАННЫХ

Каналы утечки памяти

Не обеспечивается монопольное владение данными их владельцу. Если субъект X имеет уровень благонадежности, такой же, как и у субъекта Y, то его данные полностью доступны и субъекту Y, а также всем субъектам с более высоким уровнем благонадежности.



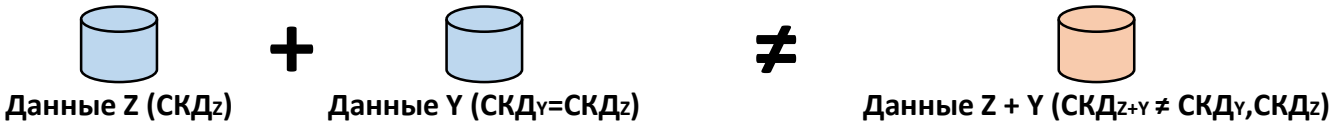
Смешение данных с разными степенями конфиденциальности в одном контейнере (документе, изделии) приводит к необходимости завышения класса конфиденциальности (по наивысшей степени) данных, которые не содержат тайну (с низкой степенью конфиденциальности).



КАНАЛЫ УТЕЧКИ В МНОГОЗНАЧНОЙ ПОДСИСТЕМЕ ЗАЩИТЫ БАЗ ДАННЫХ

Каналы утечки памяти

Концепция не позволяет изменить степень конфиденциальности данных «по совокупности сведений», если такая необходимость возникнет.



Каналы утечки времени

Время передачи строки 1 не равно времени передачи строки 2 (обусловлено необходимостью передачи разного числа байтов). Это является признаком подмены реальных данных маскирующими.

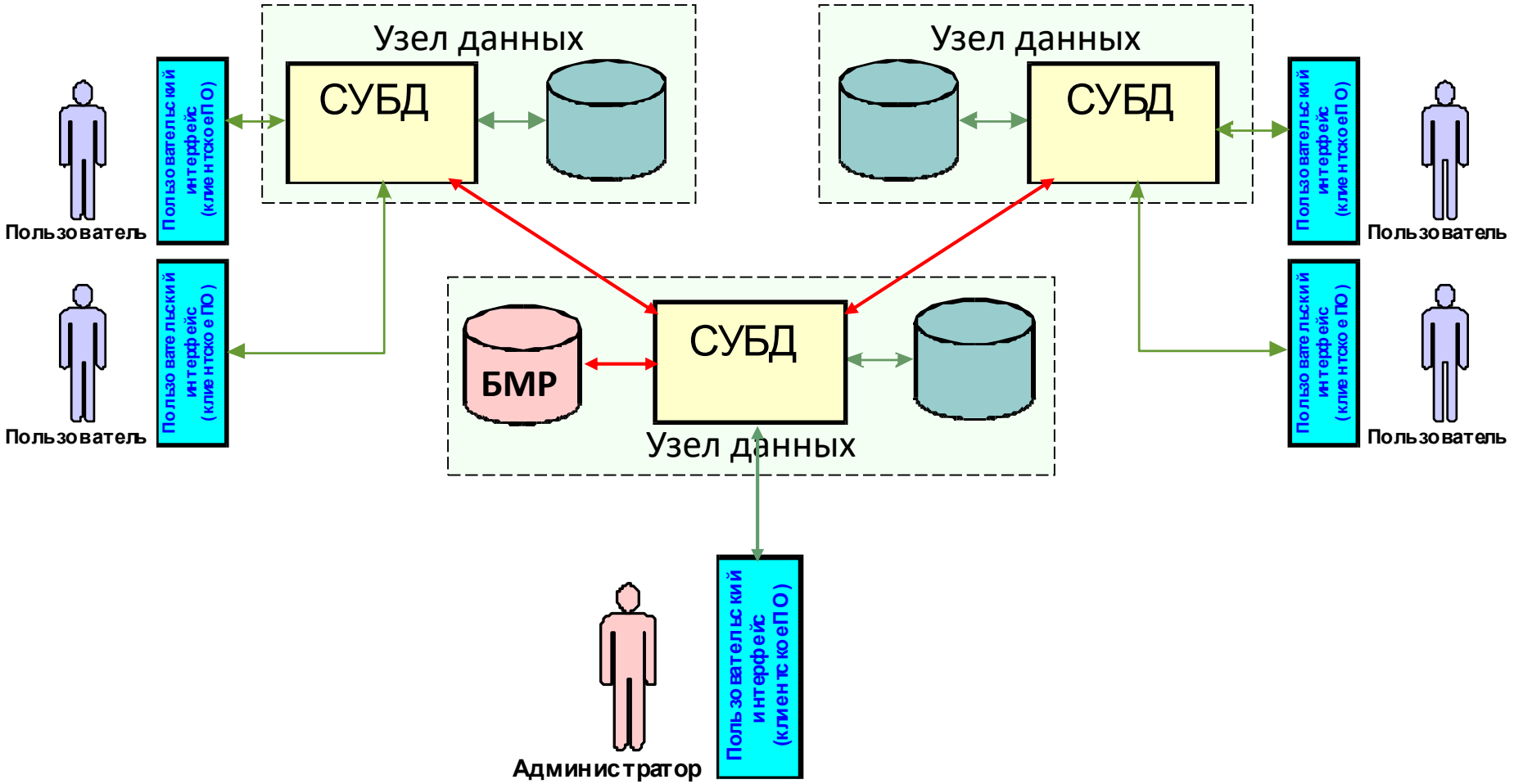
Максимов А.В.	Ambassador Extraordinary	16.03.2019	500	2
Максимов А.В.	Офицер по вербовке	16.03.2019	102	1

$$V_{\text{строки1}} \neq V_{\text{строки2}}$$

Время выборки строки неоправданно высокое, что требуется для выполнения процесса подмены реальных данных маскирующими.

Увеличение или уменьшение времени передачи данных одного и того же объекта базы данных (таблицы, представления, индекса) между субъектами с одинаковым УБП свидетельствует об изменениях в хранимых конфиденциальных данных.

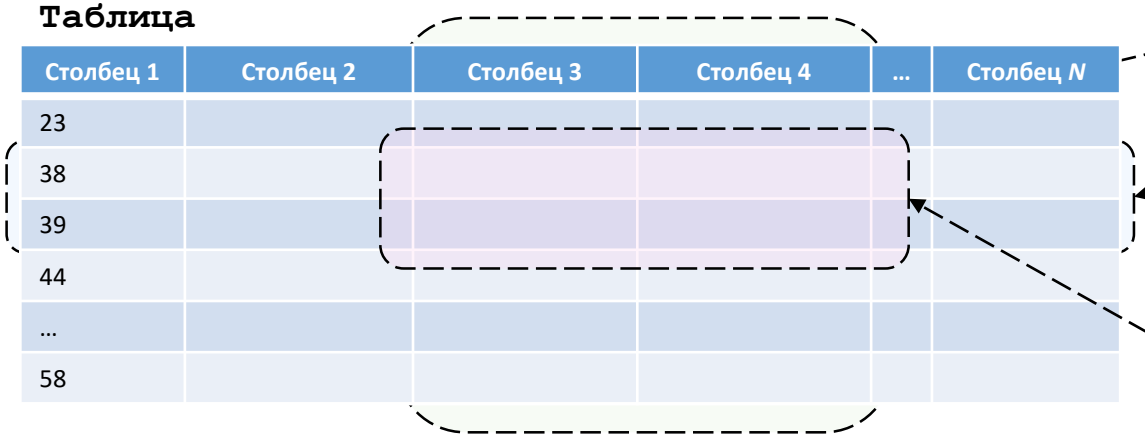
АРХИТЕКТУРА SD-DBMS С ПЕРЕАДРЕСАЦИЕЙ ЗАПРОСОВ



АРХИТЕКТУРА SD-DBMS С ПЕРЕАДРЕСАЦИЕЙ ЗАПРОСОВ

Фрагментация

Таблица



Вертикальная фрагментация:

```
SELECT "Столбец 3", "Столбец 4" FROM "Таблица";
```

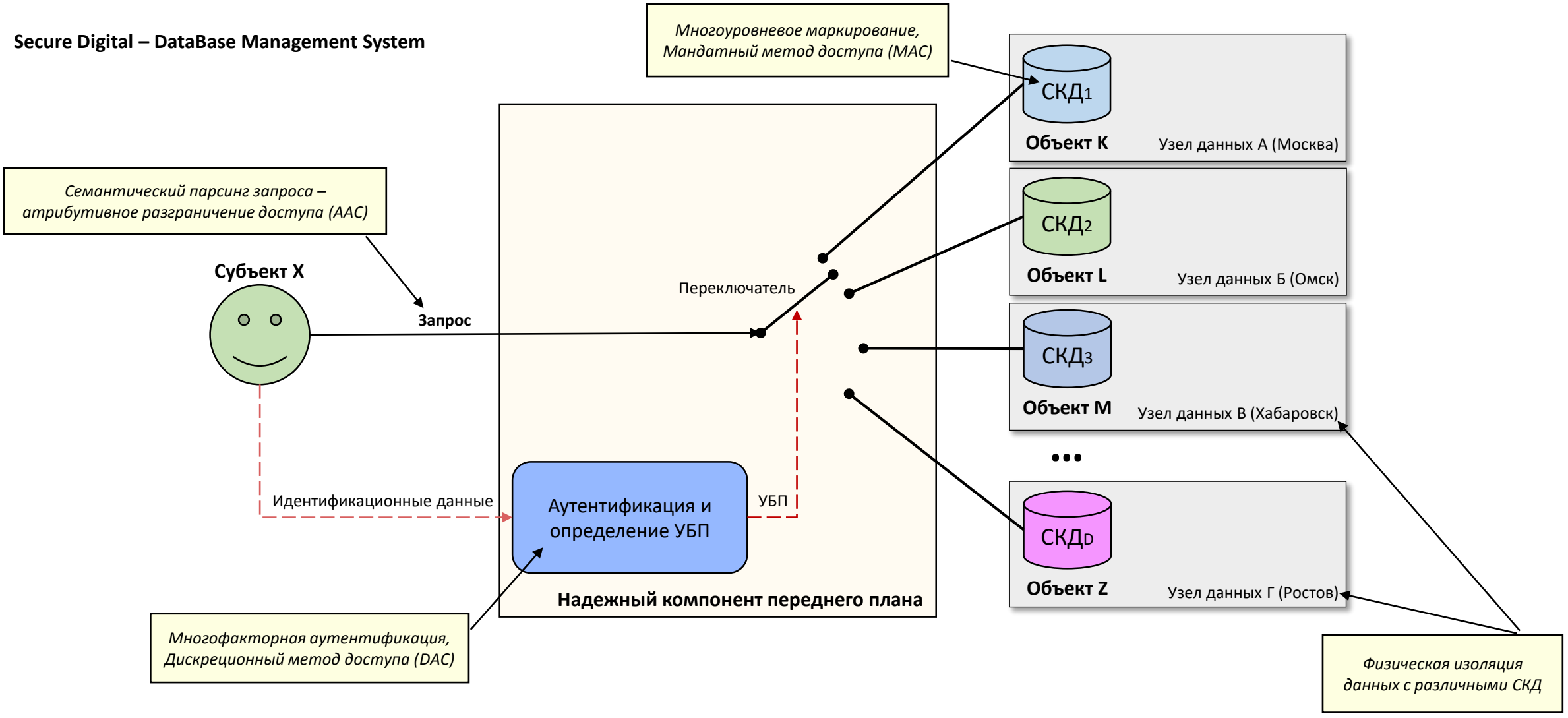
Горизонтальная фрагментация:

```
SELECT * FROM "Таблица"
         WHERE Столбец 1 BETWEEN 30 AND 39;
```

Гибридная фрагментация:

```
SELECT "Столбец 3", "Столбец 4"
         FROM "Таблица"
         WHERE Столбец 1 BETWEEN 30 AND 39;
```

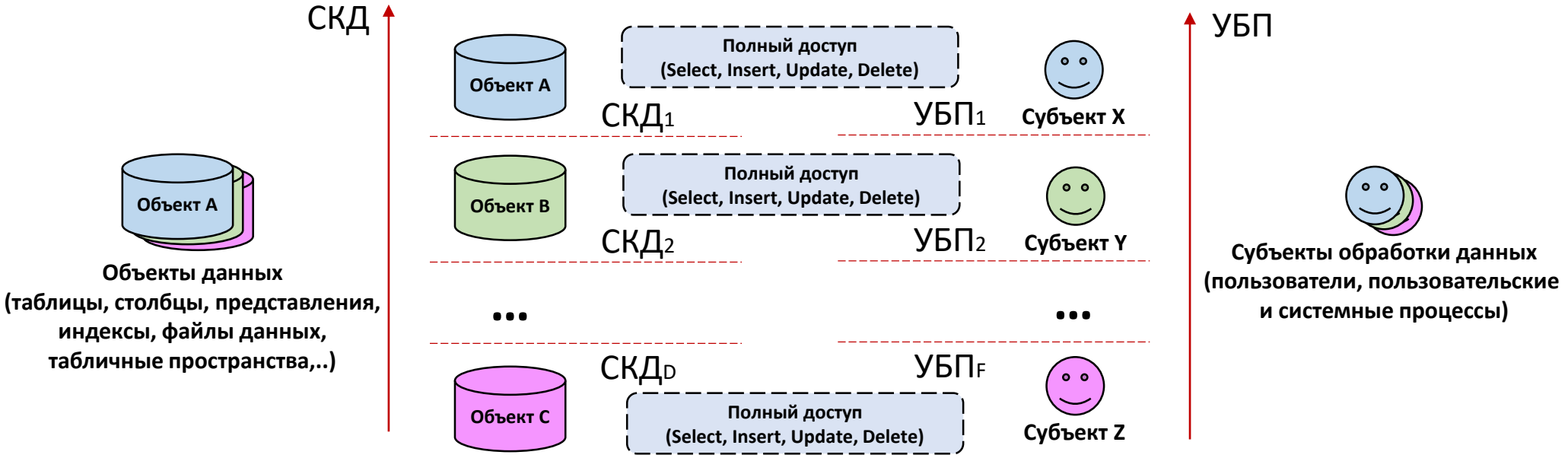
АРХИТЕКТУРА SD-DBMS С ПЕРЕАДРЕСАЦИЕЙ ЗАПРОСОВ



АРХИТЕКТУРА SD-DBMS С ПЕРЕАДРЕСАЦИЕЙ ЗАПРОСОВ

Организация защиты базы данных в соответствии с архитектурой SD – DBMS

1. Разметка данных и субъектов обработки в соответствии со степенями конфиденциальности и уровнями благонадежности. Построение системы соответствия СКД уровням благонадежности.

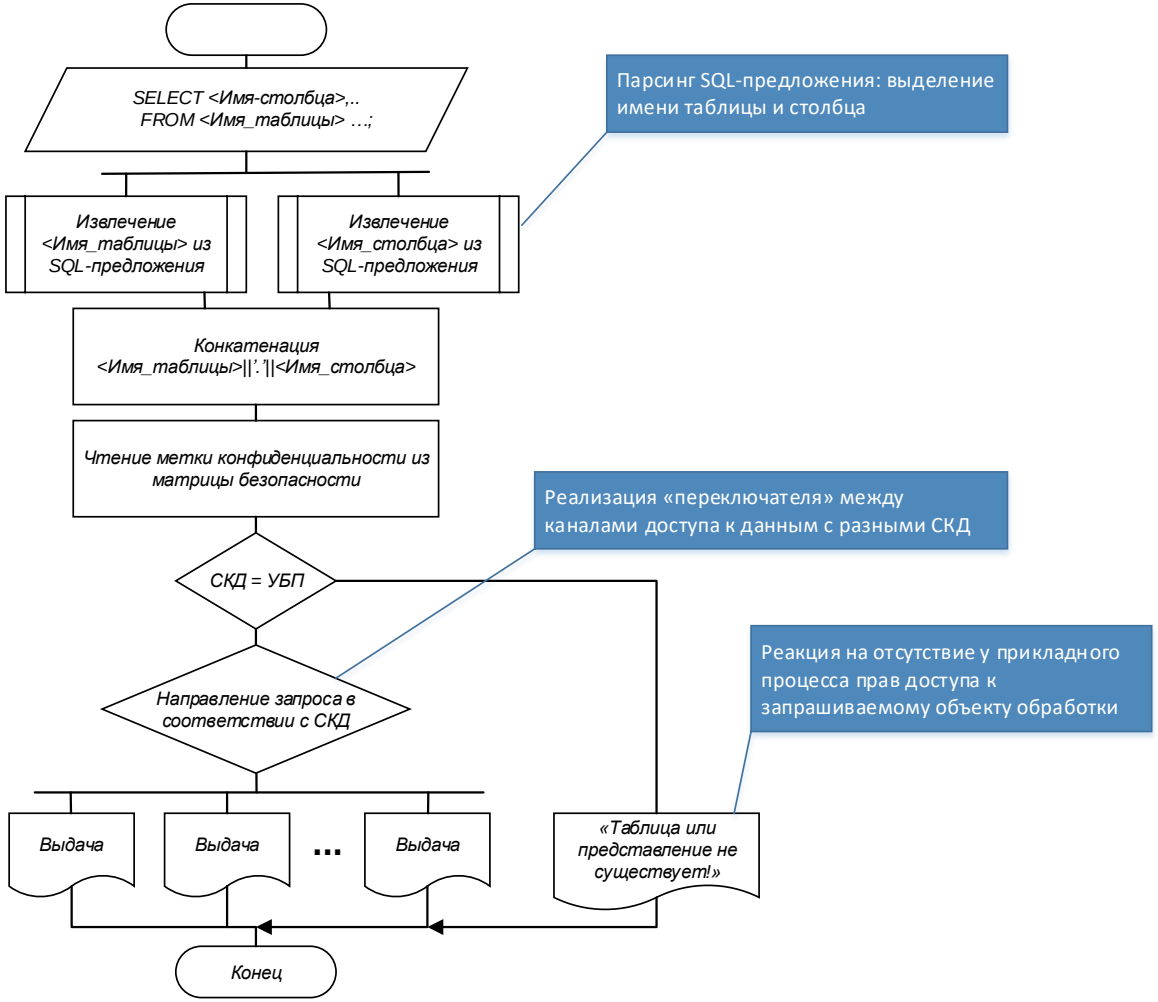


2. Организация многофакторной аутентификации и распознавания УБП субъекта обработки.

АРХИТЕКТУРА SD-DBMS С ПЕРЕАДРЕСАЦИЕЙ ЗАПРОСОВ

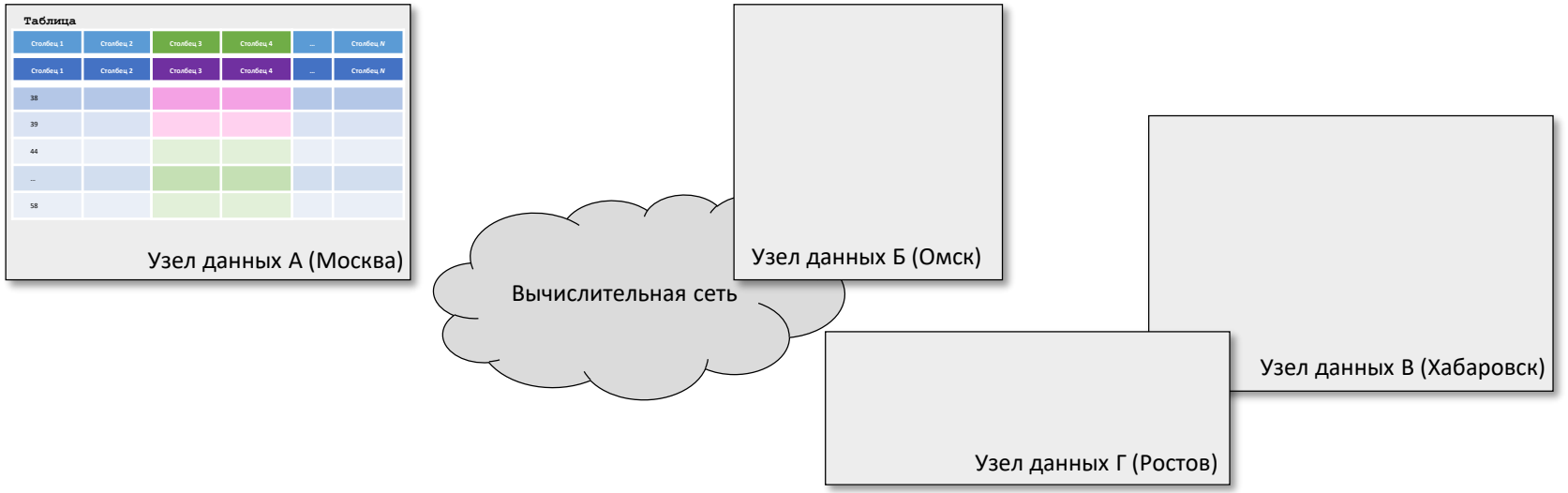
3. Разработка хранимой процедуры семантического парсинга запроса для выделения СКД набора атрибутов и перенаправления запроса в соответствии с меткой конфиденциальности.

```
CREATE [OR REPLACE] PROCEDURE
  <Имя_процедуры> (<Имя_аргумента> IN | OUT <Тип>,
                   <Имя_аргумента> IN | OUT <Тип>,..)
AS
<Метка>
  DECLARE
-- Область объявления локальных переменных
    <Имя_переменной> <Тип>;
    …;
  BEGIN
-- Область операторов алгоритма процедуры
    <Легальный_оператор>;
    …;
  EXCEPTION
-- Область описания исключений
    <Условие_завершения>;
    …:
  END;
<Метка> LANGUAGE <Имя_языка_процедуры>;
```



АРХИТЕКТУРА С ТИРАЖИРОВАНИЕМ

Тиражирование и репликация

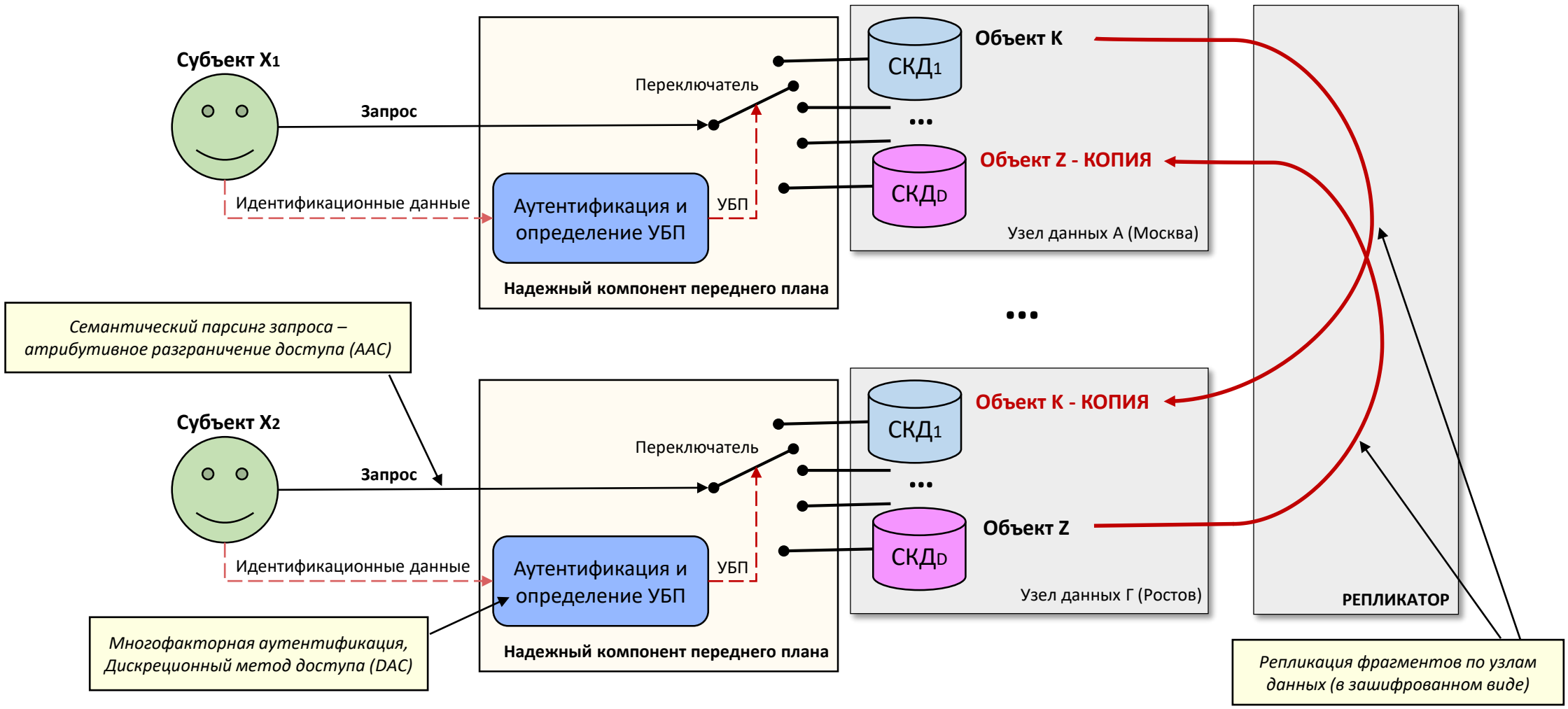


Способы репликации:

по расписанию (в периоды наименьшей нагрузки на СУБД и телекоммуникацию);
по событию (факту достижения объема накопления);
по требованию (перед выполнением критически важной транзакции).

АРХИТЕКТУРА С ТИРАЖИРОВАНИЕМ

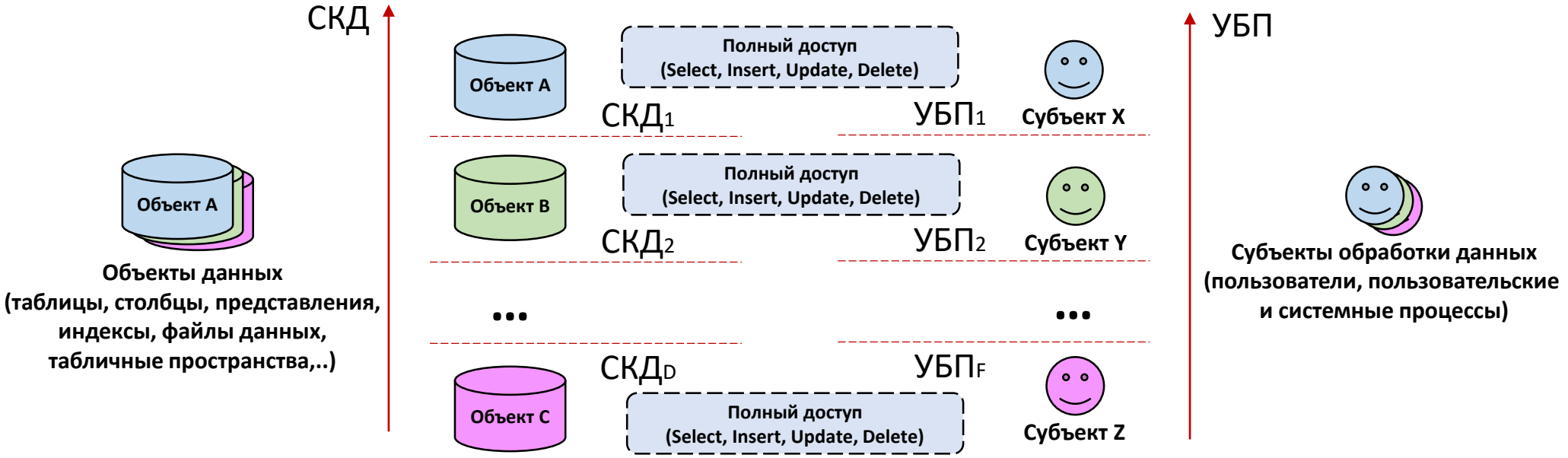
DataBase Management System with Replication



АРХИТЕКТУРА С ТИРАЖИРОВАНИЕМ

Организация защиты базы данных в соответствие с архитектурой с тиражированием

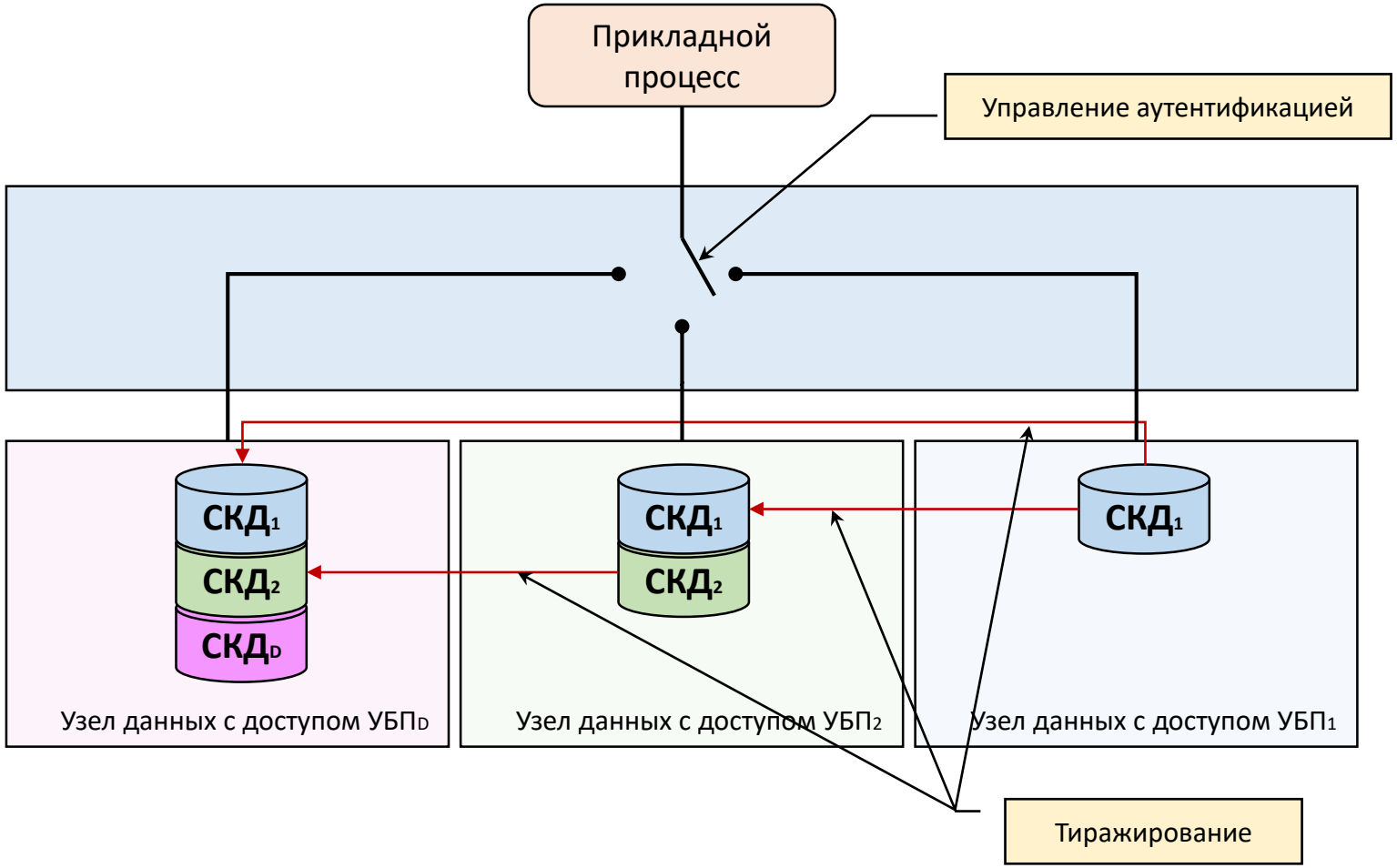
1. Разметка данных и субъектов обработки в соответствие со степенями конфиденциальности и уровнями благонадежности. Построение системы соответствия СКД уровням благонадежности.



2. Организация многофакторной аутентификации и распознавания УБП субъекта обработки.

АРХИТЕКТУРА С ТИРАЖИРОВАНИЕМ

3. Разработка хранимой процедуры семантического парсинга запроса для выделения СКД набора атрибутов.
4. Тиражирование копий фрагментов данных в подсхемы пользователей (создание реплик – снимков, *англ.* SNAPSHOT).



5. Настройка репликации снимков.

Литература:

1. **Смирнов, С. Н.** Безопасность систем баз данных [Текст]: учеб. пособие для вузов по специальностям в области информационной безопасности. – М.: Гелиос АРВ , 2007. – 350 с.

2. **Федин, Ф. О.** Информационная безопасность баз данных. Ч. 1 [Электронный ресурс]: учебное пособие / Ф. О. Федин, О. В. Трубиенко, С. В. Чискидов. — М.: РТУ МИРЭА, 2020. — Электрон. опт. диск (ISO)

3. **Саймон, А. Р.** Стратегические технологии баз данных: менеджмент на 2000 год: Пер. с англ. /Под ред. и с предисл. М. Р. Когаловского. - М.: Финансы и статистика, 1999 - 479 с.: ил.

4. **Терьо, М.** Oracle. Руководство по безопасности [Текст] / М. Терьо, А. Ньюмен; Пер. с англ.. — М.: Лори, 2004. — 560 с.: ил.

5. **Кузнецов, С. Д.** Основы баз данных: курс лекций : учеб. пособие для студентов вузов, обучающихся по специальностям в обл. ин-форм. технологий / С. Д. Кузнецов. – Москва: Интернет-ун-т ин-форм. технологий, 2005. – 488 с.

6. **Смирнов, С. Н., Задворьев, И. С.** Работаем с ORACLE.: Учебное пособие/2-е изд., испр. и доп. – М: Гелиос АРВ, 2002 г. – 496 с.

7. **Кульба, В.В.** и др. Теоретические основы проектирования оптимальных структур распределенных баз данных. – М: СИНТЕГ, 1999 г. – 660 с.

8. Материалы сервера ORACLE/RE. www.oracle.ru/press/magazine/main.html

9. Материалы информационного ресурса WIKIPEDIA. https://ru.wikipedia.org/wiki/Разграничение_доступа_на_основе_атрибутов; https://ru.wikipedia.org/wiki/Аутентификация; https://ru.wikipedia.org/wiki/Многофакторная_аутентификация; https://ru.wikipedia.org/wiki/Сложность_пароля.

10. Материалы информационного ресурса http://www.nsc.ru/ws/YM2003/6299/